

# Information Security Management ISO 17799:2005 Audit Checklist

Checklist	ISO 17799 (2005)	Section	Audit Question	Results	
<b>1</b>	<b>5</b>	<b>SECURITY POLICY</b>		<b>Findings</b>	<b>Compliance</b>
1.1	5.1	INFORMATION SECURITY POLICY			

The information security policy document should state management commitment and set out the organization's approach to managing information security. The policy document should contain statements concerning:

a) A definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);

b) A statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;

c) A framework for setting control objectives and controls, including the structure of risk assessment and risk management;

d) A brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:

1) Compliance with legislative, regulatory, and contractual requirements;

2) Security education, training, and awareness requirements;

3) Business continuity management;

4) Consequences of information security policy violations;

e) A definition of general and specific responsibilities for information security management, including reporting information security incidents;

1.1.2	5.1.2	Review of the information security policy	<p>The information security policy should have an owner who has approved management responsibility for the development, review, and evaluation of the security policy. The review should include assessing opportunities for improvement of the organization's information security policy and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions, or technical environment.</p> <p>The review of the information security policy should take account of the results of management reviews. There should be defined management review procedures, including a schedule or period of the review.</p> <p>A record of the management review should be maintained.</p> <p>Management approval for the revised policy should be obtained.</p>		
<b>2</b>	<b>6</b>	<b>ORGANIZATION OF INFORMATION SECURITY</b>			
2.1	6.1	INTERNAL ORGANIZATION			

2.1.1	6.1.1	Management commitment to information security	<p>Management should:</p> <ul style="list-style-type: none"> <li>a) Ensure that information security goals are identified, meet the organizational requirements, and are integrated in relevant processes;</li> <li>b) Formulate, review, and approve information security policy;</li> <li>c) Review the effectiveness of the implementation of the information security policy;</li> <li>d) Provide clear direction and visible management support for security initiatives;</li> <li>e) Provide the resources needed for information security;</li> <li>f) Approve assignment of specific roles and responsibilities for information security across the organization;</li> <li>g) Initiate plans and programs to maintain information security awareness;</li> <li>h) Ensure that the implementation of information security controls is coordinated across the organization (see 6.1.2).</li> </ul> <p>Management should identify the needs for internal or external specialist information security advice, and review and coordinate results of the advice throughout the organization.</p> <p>Depending on the size of the organization, such responsibilities could be handled by a dedicated management forum or by an existing management body, such as the board of directors.</p>		
-------	-------	---	--	--	--

2.1.2	6.1.2	Information security co-ordination	Information security activities should be coordinated by representatives from different parts of the organization with relevant roles and job functions.			
2.1.3	6.1.3	Allocation of information security responsibilities	All information security responsibilities should be clearly defined.			
2.1.4	6.1.4	Authorization process for information processing facilities	A management authorization process for new information processing facilities should be defined and implemented.			
2.1.5	6.1.5	Confidentiality agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.			
2.1.6	6.1.6	Contact with authorities	Appropriate contacts with relevant authorities should be maintained.			
2.1.7	6.1.7	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.			
2.1.8	6.1.8	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.			
2.1.9						
2.2	6.2	EXTERNAL PARTIES				

2.2.1	6.2.1	Identification of risks related to external parties	The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access			
2.2.2	6.2.2	Addressing security when dealing with customers	All identified security requirements should be addressed before giving customers access to the organization's information or assets.			
2.2.3	6.2.3	Addressing security in third party agreements	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.			
<b>3</b>	<b>7</b>	<b>ASSET MANAGEMENT</b>				
3.1	7.1	RESPONSIBILITY FOR ASSETS				
3.1.1	7.1.1	Inventory of assets	All assets should be clearly identified and an inventory of all important assets drawn up and maintained.			
3.1.2	7.1.2	Ownership of assets	All information and assets associated with information processing facilities should be owned <sup>2</sup> by a designated part of the organization.			
3.1.3	7.1.3	Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.			
<b>3.2</b>	<b>7.2</b>	<b>INFORMATION CLASSIFICATION</b>				

3.2.1	7.2.1	Classification guidelines	Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.		
3.2.2	7.2.2	Information labeling and handling	An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.		
<b>4</b>	<b>8</b>	<b>HUMAN RESOURCES SECURITY</b>			
4.1	8.1	PRIOR TO EMPLOYMENT			
4.1.1	8.1.1	Roles and responsibilities	An association's security policy must define and document the roles and duties of all employees, contractors, and external users.		
4.1.2	8.1.2	Screening	All potential employees, contractors, and external users should have extensive background checks ran in accordance with applicable laws, regulations, and ethics. All accessed information should be considered confidential		
4.1.3	8.1.3	Terms and conditions of employment	All employees, contractors, and external users must sign an employment contract that defines their responsibilities for information security		
4.2	8.2	DURING EMPLOYMENT			
4.2.1	8.2.1	Management responsibilities	All employees, contractors, and external users must apply their organization's security practices based on their explicit policy.		

4.2.2	8.2.2	Information security awareness, education, and training	Regular training and updates must be scheduled for all employees, contractors, and external users on security policies and procedure		
4.2.3	8.2.3	Disciplinary process	Disciplinary procedures must be documented and implemented for any employee who commits a security breach		
4.3	8.3	TERMINATION OR CHANGE OF EMPLOYMENT			
4.3.1	8.3.1	Termination responsibilities	Procedures for employment changes or termination should be defined and assigned to appropriate staff members.		
4.3.2	8.3.2	Return of assets	All employees, contractors, and external users must return all property owned by the organization upon termination of employment.		
4.3.3	8.3.3	Removal of access rights	Access to an organization's information and facilities must be eradicated upon termination of employment for all employees, contractors, and external users.		
<b>5</b>	<b>9</b>	<b>PHYSICAL AND ENVIRONMENTAL SECURITY</b>			
5.1	9.1	SECURE AREAS			
5.1.1	9.1.1	Physical security perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.		

5.1.2	9.1.2	Physical entry controls	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.		
5.1.3	9.1.3	Securing offices, rooms, and facilities	Physical security for offices, rooms, and facilities should be designed and applied		
5.1.4	9.1.4	Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.		
5.1.5	9.1.5	Working in secure areas	Physical protection and guidelines for working in secure areas should be designed and applied.		
5.1.6	9.1.6	Public access, delivery, and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.		
5.2	9.2	<b>EQUIPMENT SECURITY</b>			
5.2.1	9.2.1	Equipment siting and protection	Equipment should be sighted or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.		
5.2.2	9.2.2	Supporting utilities	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.		
5.2.3	9.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.		

5.2.4	9.2.4	Equipment maintenance	Equipment should be correctly maintained to ensure its continued availability and integrity.			
5.2.5	9.2.5	Security of equipment off-premises	Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises.			
5.2.6	9.2.6	Secure disposal or re-use of equipment	All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.			
5.2.7	9.2.7	Removal of property	Equipment, information or software should not be taken off-site without prior authorization.			
<b>6</b>	<b>10</b>	<b>COMMUNICATIONS AND OPERATIONS MANAGEMENT</b>				
6.1	10.1	OPERATIONAL PROCEDURES AND RESPONSIBILITIES				
6.1.1	10.1.1	Documented operating procedures	Operating procedures should be documented, maintained, and made available to all users who need them.			
6.1.2	10.1.2	Change management	Changes to information processing facilities and systems should be controlled.			
6.1.3	10.1.3	Segregation of duties	Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.			

6.1.4	10.1.4	Separation of development, test, and operational facilities	Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.			
6.2	10.2	<b>THIRD PARTY SERVICE DELIVERY MANAGEMENT</b>				
6.2.1	10.2.1	Service delivery	It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.			
6.2.2	10.2.2	Monitoring and review of third party services	The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.			
6.2.3	10.2.3	Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.			
6.3	10.3	<b>SYSTEM PLANNING AND ACCEPTANCE</b>				
6.3.1	10.3.1	Capacity management	The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance			
6.3.2	10.3.2	System acceptance	Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance			

6.4	10.4	PROTECTION AGAINST MALICIOUS AND MOBILE CODE			
6.4.1	10.4.1	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.		
6.4.2	10.4.2	Controls against mobile code	Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.		
6.5	10.5	BACK-UP			
6.5.1	10.5.1	Information back-up	Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.		
6.6	10.6	NETWORK SECURITY MANAGEMENT			
6.6.1	10.6.1	Network controls	Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.		
6.6.2	10.6.2	Security of network services	Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.		
6.7	10.7	MEDIA HANDLING			
6.7.1	10.7.1	Management of removable media	There should be procedures in place for the management of removable media.		
6.7.2	10.7.2	Disposal of media	Media should be disposed of securely and safely when no longer required, using formal procedures.		
6.7.3	10.7.3	Information handling procedures	Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.		

6.7.4	10.7.4	Security of system documentation	System documentation should be protected against unauthorized access.		
6.8	10.8	<b>EXCHANGE OF INFORMATION</b>			
6.8.1	10.8.1	Information exchange policies and procedures	Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities		
6.8.2	10.8.2	Exchange agreements	Agreements should be established for the exchange of information and software between the organization and external parties.		
6.8.3	10.8.3	Physical media in transit	Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.		
6.8.4	10.8.4	Electronic messaging	Information involved in electronic messaging should be appropriately protected.		
6.8.5	10.8.5	Business information systems	Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.		
6.9	10.9	<b>ELECTRONIC COMMERCE SERVICES</b>			
6.9.1	10.9.1	Electronic commerce	Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.		
6.9.2	10.9.2	On-Line Transactions	Information involved in on-line transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay		
6.9.3	10.9.3	Publicly available information	The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification		

6.10	10.10	MONITORING			
6.10.1	10.10.1	Audit logging	Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.		
6.10.2	10.10.2	Monitoring system use	Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.		
6.10.3	10.10.3	Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.		
6.10.4	10.10.4	Administrator and operator logs	System administrator and system operator activities should be logged.		
6.10.5	10.10.5	Fault logging	Faults should be logged, analyzed, and appropriate action taken.		
6.10.6	10.10.6	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.		
<b>7</b>	<b>11</b>	<b>ACCESS CONTROL</b>			
7.1	11.1	BUSINESS REQUIREMENT FOR ACCESS CONTROL			
7.1.1	11.1.1	Access control policy	An access control policy should be established, documented, and reviewed based on business and security requirements for access.		
7.2	11.2	USER ACCESS MANAGEMENT			
7.2.1	11.2.1	User registration	There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services		

7.2.2	11.2.2	Privilege management	The allocation and use of privileges should be restricted and controlled.		
7.2.3	11.2.3	User password management	The allocation of passwords should be controlled through a formal management process		
7.2.4	11.2.4	Review of user access rights	Management should review users' access rights at regular intervals using a formal process.		
7.3	11.3	<b>USER RESPONSIBILITIES</b>			
7.3.1	11.3.1	Password use	Users should be required to follow good security practices in the selection and use of passwords.		
7.3.2	11.3.2	Unattended user equipment	Users should ensure that unattended equipment has appropriate protection		
7.3.3	11.3.3	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.		
7.4	11.4	<b>NETWORK ACCESS CONTROL</b>			
7.4.1	11.4.1	Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorized to use.		
7.4.2	11.4.2	User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.		
7.4.3	11.4.3	Equipment identification in networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.		
7.4.4	11.4.4	Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports should be controlled.		
7.4.5	11.4.5	Segregation in networks	Groups of information services, users, and information systems should be segregated on networks.		
7.4.6	11.4.6	Network connection control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications		

7.4.7	11.4.7	Network routing control	Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.			
7.5	11.5	OPERATING SYSTEM ACCESS CONTROL				
7.5.1	11.5.1	Secure log-on procedures	Access to operating systems should be controlled by a secure log-on procedure.			
7.5.2	11.5.2	User identification and authentication	All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.			
7.5.3	11.5.3	Password management system.	Systems for managing passwords should be interactive and should ensure quality passwords.			
7.5.4	11.5.4	Use of system utilities	The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.			
7.5.5	11.5.5	Session time-out	Inactive sessions should shut down after a defined period of inactivity.			
7.5.6	11.5.6	Limitation of connection time	Restrictions on connection times should be used to provide additional security for high-risk applications			
7.6	11.6	APPLICATION AND INFORMATION ACCESS CONTROL				
7.6.1	11.6.1	Information access restriction .	Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.			
7.6.2	11.6.2	Sensitive system isolation	Sensitive systems s should have a dedicated (isolated) computing environment			
7.7	11.7	MOBILE COMPUTING AND TELEWORKING				

7.7.1	11.7.1	Mobile computing and communications	A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.		
7.7.2	11.7.2	Teleworking	A policy, operational plans and procedures should be developed and implemented for telecommuting activities		
<b>8</b>	<b>12</b>	<b>SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTANANCE</b>			
8.1	12.1	SECURITY REQUIREMENTS OF INFORMATION SYSTEMS			
8.1.1	12.1.1	Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.		
8.2	12.2	CORRECT PROCESSING IN APPLICATIONS			
8.2.1	12.2.1	Input data validation	Data input to applications should be validated to ensure that this data is correct and appropriate		
8.2.2	12.2.2	Control of internal processing.	Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts		
8.2.3	12.2.3	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented		
8.2.4	12.2.4	Output data validation	Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances		
8.3	12.3	CRYPTOGRAPHIC CONTROLS			

8.3.1	12.3.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information should be developed and implemented.			
8.3.2	12.3.2	Key management	Key management should be in place to support the organization's use of cryptographic techniques.			
8.4	12.4	<b>SECURITY OF SYSTEM FILES</b>				
8.4.1	12.4.1	Control of operational software	There should be procedures in place to control the installation of software on operational systems.			
8.4.2	12.4.2	Protection of system test data..	Test data should be selected carefully, and protected and controlled.			
8.4.3	12.4.3	Access control to program source code	Access to program source code should be restricted.			
8.5	12.5	<b>SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES</b>				
8.5.1	12.5.1	Change control procedures	The implementation of changes should be controlled by the use of formal change control procedures.			
8.5.2	12.5.2	Technical review of applications after operating system changes	When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.			
8.5.3	12.5.3	Restrictions on changes to software packages	Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.			
8.5.4	12.5.4	Information leakage	Opportunities for information leakage should be prevented.			
8.5.5	12.5.5	Outsourced software development	Outsourced software development should be supervised and monitored by the organization.			
8.6	12.6	<b>TECHNICAL VULNERABILITY MANAGEMENT</b>				

8.6.1	12.6.1	Control of technical vulnerabilities	Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.			
<b>9</b>	<b>13</b>	<b>INCIDENT MANAGEMENT</b>				
9.1	13.1	REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES				
9.1.1	13.1.1	Reporting information security events	All information security events and incidents must be reported as quickly as possible to appropriate management.			
9.1.2	13.1.2	Reporting security weaknesses	All personnel using any information systems and services are required to report any perceived security weaknesses			
9.2	13.2	MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS				
9.2.1	13.2.1	Responsibilities and procedures	The responsibilities and expectations of management should be established to provide fast and efficient responses to information security incidents and events.			
9.2.2	13.2.2	Learning from information security incidents	Metrics should be used to identify and monitor the types, quantities and costs of security incidents.			
9.2.3	13.2.3	Collection of evidence	Evidence of an information security incident should always be collected, preserved, and presented in accordance to rules for evidence established in the relevant jurisdiction, regardless as to whether any legal action will be taken			

<b>10</b>	<b>14</b>	<b>BUSINESS CONTINUITY MANAGEMENT</b>			
10.1	14.1	INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT			
10.1.1	14.1.1	Including information security in the business continuity management process	A managed process should be developed and implemented for business continuity within an organization that establishes the information security requirements necessary for the stability of the organization and its business.		
10.1.2	14.1.2	Business continuity and risk assessment	Identify events that can cause interruptions to an organization, and the likelihood and impact of such interruptions and their effects on information security.		
10.1.3	14.1.3	Developing and implementing continuity plans including information security	Continuity plans should be established to securely restore business operations and information availability in an acceptable time-frame following any interruptions to critical business processes		
10.1.4	14.1.4	Business continuity planning framework	Business continuity plans should be maintained for consistency in all areas, including information security requirements and identifying priorities for testing and maintenance.		
10.1.5	14.1.5	Testing, maintaining and re-assessing business continuity plans	Business continuity plans should be regularly tested, evaluated and updated to ensure that they remain current and effective.		
<b>11</b>	<b>15</b>	<b>COMPLIANCE</b>			
11.1	15.1	COMPLIANCE WITH LEGAL REQUIREMENTS			

11.1.1	15.1.1	Identification of applicable legislation	All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.		
11.1.2	15.1.2	Intellectual property rights (IPR)	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.		
11.1.3	15.1.3	Protection of organizational records	Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements		
11.1.4	15.1.4	Data protection and privacy of personal information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.		
11.1.5	15.1.5	Prevention of misuse of information processing facilities	Users should be deterred from using information processing facilities for unauthorized purposes		
11.1.6	15.1.6	Regulation of cryptographic controls	Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations.		
11.2	15.2	COMPLIANCE WITH SECURITY POLICIES & STANDARDS, & TECHNICAL COMPLIANCE			
11.2.1	15.2.1	Compliance with security policies and standards	Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.		

11.2.2	15.2.2	Technical compliance checking	Information systems should be regularly checked for compliance with security implementation standards.		
11.3	15.3	<b>INFORMATION SYSTEMS AUDIT CONSIDERATIONS</b>			
11.3.1	15.3.1	Information systems audit controls	Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes.		
11.3.4	15.3.2	Protection of information systems audit tools	Access to information systems audit tools should be protected to prevent any possible misuse or compromise.		